Michigan Cyber Initiative

Defense and Development for Michigan Citizens, Businesses and Industry

Letter From The Governor

The Internet's impact on our world continues to be profound. Whether we're chatting with friends, accessing government services or conducting global commerce, opportunities abound to enhance our daily lives through the convenience and speed afforded by technology.

Unfortunately, the Internet also provides new avenues for crime, misconduct and espionage. Last year alone, 8 million people reported cases of identity theft. More than $1 trillion in commerce has been lost and terabytes of data have been stolen or compromised.

In an equally disturbing trend, these crimes are now the province of professionals. Amateur "hacking" has given way to organized, sophisticated attacks on our personal safety and economic security.

Against that backdrop, Michigan is taking a leadership role in cyber defense and development for Michigan's citizens, businesses and industry. The Michigan Cyber Initiative is focused on protecting the vulnerable ecosystem in the cyber world.

This report underscores Michigan's commitment to cybersecurity. It is an action plan that offers clear approaches for safeguarding our families, protecting Michigan's infrastructure and shielding our economy. In keeping with Michigan's innovative spirit, these pages also outline ways in which our state will seize the economic opportunities spawned by the burgeoning field of cybersecurity.

Technology is Michigan's future. Our already heavy reliance on the Internet will only grow, making it imperative that we treat the issue of cybersecurity with the urgency it deserves.

I'm proud that once again, Michigan is taking a visionary, proactive approach to meeting its challenges and embracing opportunities. By working together, our state will be a national model of innovation, success and security.

Rick Snyder
Governor
State of Michigan

Michigan Cyber Initiative
Defense and Development for Michigan Citizens, Businesses and Industry

EXECUTIVE SUMMARY

The Internet has changed everything. With a few keystrokes, friends are updated, a driver's license is renewed, a credit card bill is paid, new parts for the production line are ordered, or electricity load demand is balanced across the grid. Or, without adequate protections, an identity is stolen, a bank account balance modified, a confidential manufacturing process is pirated or the power grid compromised.

Michigan, along with the entire global economy, relies on information technology and systems. This broad and complex system involves every aspect of the economy, and the very technologies that make lives more convenient can also leave us more vulnerable.

Unfortunately, this information ecosystem has created a new avenue for crime, misconduct and espionage. Over 8 million people nationwide reported cases of identity theft last year costing over $37 billion. Over $1 trillion in commerce has been lost and terabytes of data have been stolen or compromised. And make no mistake; these attacks are now the province of professionals.

As individuals, businesses and governments increasingly conduct their lives online, Michigan's future demands a secure cyber ecosystem that safeguards citizens, protects critical infrastructure and defends intellectual properties.

Michigan's vision is to secure this ecosystem and to continue its leadership in this domain. The Michigan Cyber Initiative is built around three distinct but equally important pillars:

CONFIDENTIALITY (ensuring private information in the ecosystem remains private)
INTEGRITY (ensuring that the information in the ecosystem is complete, whole and defensibly sound)
AVAILABILITY (ensuring that the information in the ecosystem continues to be available to serve its purpose)

This approach will extend to all components of our ecosystem: home users, small businesses, communities, large commercial enterprises and critical infrastructure.

This initiative is for everyone because cyber systems affect all of our lives. Cyber crime has a subtle but serious impact on each and every component of the ecosystem.

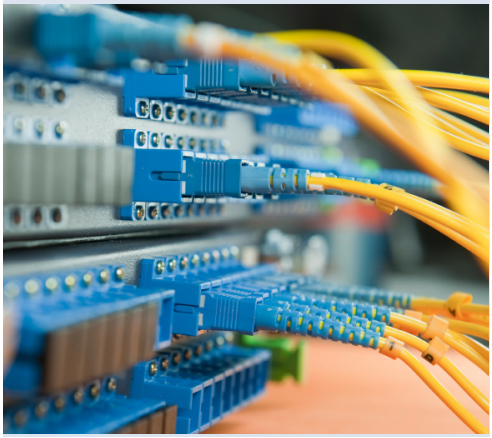
>>Facts on Cyber Attacks

Each Day in 2010, Michigan state government averaged:

- 29,942 blocked web browser attacks
- 24,671 blocked web site attacks
- 14,072 blocked network scans
- 88,774 blocked intrusion attempts

In 2010, national statistics showed:

- 79.9% of websites with malicious code were legitimate sites that were compromised
- 89.9% of all unwanted emails in circulation during this period contained links to spam sites or malicious websites
- 52% of data stealing attacks occurred over the web
- Data theft and breaches from cyber crime may cost businesses as much as $1 trillion globally



Michigan Cyber Initiative
Defense and Development for Michigan Citizens, Businesses and Industry

Elements of Michigan's Cyber Threat Response

Just as invasive species threaten biological ecosystems around the globe, cyber attacks pose a real and serious hazard to our safety and security. Both situations can result in long-term implications that are costly and often produce irreversible damage. Therefore, Michigan is approaching cybersecurity with the same level of commitment when preparing for and responding to threats to the natural environment:

- **Prevention** – taking steps to keep an event from happening
- **Early Detection and Rapid Response** – discovering an attack in its early stages and responding to minimize the consequences
- **Control, Management and Restoration** – taking appropriate steps to minimize and contain the effects of an event and return to normal operations

Through continued research, education and collaboration in these areas, the state of Michigan will positively leverage its people, businesses and technology expertise to deter and prevent attacks against our digital infrastructure.

With proper execution, each of these elements will secure our cyber ecosystem, enhance Michigan's leadership in this critical 21st century arena and provide new economic development opportunities in our state.

Michigan's Unique Cyber Industry Opportunity

Michigan is positioned to lead the next generation of cyber security initiatives. The talent and resources available in Michigan were instrumental in building and advancing the Internet's technology, with the backbone of Internet2 being designed and introduced first in southeast Michigan. Additionally, the state has a long history of building partnerships with the federal government, law enforcement and the private sector that is the foundation for future collaboration.

Michigan possesses access to the talent and capital that are critical for researching, designing and testing technology in a timely and effective manner. Michigan's universities are among the world's leaders in information technology research and development, with five colleges and universities designated by the National Security Agency (NSA) as "National Centers of Academic Excellence in Information Assurance." Furthermore, Michigan recently launched a $3 billion public-private initiative called "Pure Michigan Business Connect" to promote a culture of innovation, linking entrepreneurs to capital.

In the pages that follow, discover more about the Michigan Cyber Initiative and what it means for families, communities, businesses and quality of life.

Five colleges and universities designated by the National Security Agency as "National Centers of Academic Excellence in Information Assurance":

Walsh College

University of Detroit Mercy

Eastern Michigan University

Davenport University

Ferris State University

Michigan Cyber Initiative
Defense and Development for
Michigan Citizens, Businesses and Industry

PART I – DEFINING CYBERSECURITY

The **MICHIGAN CYBER INITIATIVE** is built upon three distinct but equally important pillars that taken together define the security concept:

CONFIDENTIALITY
(ensuring private information in the ecosystem remains private)

INTEGRITY
(ensuring that the information in the ecosystem is complete, whole and defensibly sound)

AVAILABILITY
(ensuring that the information in the ecosystem continues to be available to serve its purpose)

The three pillars apply to all of the components of our ecosystem. The following chart provides examples that affect everyday life:

Ecosystem Component	Confidentiality	Integrity	Availability
Homes, Individuals, Small Businesses & Schools	Confidential medical records should be released only to those people or organizations (i.e., doctor, hospital, insurance, government agency, etc.) authorized to review them.	The records should be well protected so that no one can change the information without authorization.	The records should be available and accessible to authorized users.
Large Industry, Government Agencies, Commercial & Academic Institutions	Technical documents regarding a research and development program for an innovative mechanical device must be safeguarded from theft by competitors or industrial espionage.	The technical specifications for a novel device must be protected from manipulation.	The information must be able to be shared with appropriate divisions within the company and with the government agency sponsoring the program.
Infrastructure (e.g., Utility Providers, Banking & Financial, & Transportation)	Information about financial accounts at a local bank must not be made available to anyone without the account owners expressed authorization.	The databases pertaining to various accounts for home and auto loans, investments, etc, must be safeguarded by financial institutions from tampering or data being divulged to unauthorized parties.	The information concerning savings, checking, loan and investment balances must be readily available to the account owner using appropriate ID and password via online systems.

Michigan Cyber Initiative
Defense and Development for
Michigan Citizens, Businesses and Industry

PART II –MICHIGAN'S CYBER THREAT RESPONSE

Prevention

Prevention is the best strategy to provide a secure cyber environment. In the cybersecurity arena, Michigan continues to develop effective prevention measures involving both government, higher education and the private sector.

State and Local Government

Michigan is a leader in implementing state government cybersecurity measures and in promoting cyber industry growth. Michigan was a leader among the states in creating a "center for excellence" in cybersecurity management. It is also the first state to create a Chief Security Officer (CSO) over cybersecurity and infrastructure protection. Additionally, the award winning website www.michigan.gov/cybersecurity has helped spread the word on cyber protection nationwide and has been expanded to include a new "toolkit" and other helpful features.

Michigan also participates in ongoing efforts to improve inter-state and federal-state coordination in cybersecurity awareness, training and education, threat prevention, response and recovery operations. Since 2003, Michigan has been a member of the Multi-State — Information-Sharing and Analysis Center (MS-ISAC). MS-ISAC is a partnership between state governments and federal agencies and centers, such as the National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security (DHS), focused on sharing and coordinating cybersecurity information. Michigan has also partnered with local governments to share real-time intelligence on cyber threats and is now manning a 24-hour cybersecurity operations center.

Due to its close working relationship with DHS, Michigan was selected as the only state to partner with the Department to deploy the EINSTEIN 1 Intrusion Detection System (IDS) on networks managed by state government. In 2009, EINSTEIN 1 was a pilot program

EINSTEIN and ALBERT Cyber Programs

What is the EINSTEIN Program? It is a cyber-traffic monitoring system designed, implemented and operated by the United States Computer Emergency Readiness Team (US-CERT) which is part of the United States Department of Homeland Security (DHS). The EINSTEIN system automates the process of collecting, correlating and analyzing cyber traffic information across the federal civilian government in order to identify unauthorized traffic.

Why was Michigan Involved in a Federal Program? In 2009, the Department of Homeland Security was evaluating how it could enhance the cyber security of non-federal critical cyber infrastructure. Because of Michigan's active cyber partnership with DHS, DHS selected Michigan to conduct a proof of concept involving how the EINSTEIN 1 system might be used by the 50 states.

What was the purpose? The sharing of the EINSTEIN 1 capability provided an opportunity for the Feds to leverage their existing federal investment in EINSTEIN 1 to enhance the cyber security of nonfederal critical cyber infrastructure in accordance with Section 223 of the Homeland Security Act, and allowed both parties to have increased awareness of the cyber security threat and protection environment.

What were the benefits of participating in the pilot for Michigan? The proof of concept benefited Michigan's cybersecurity interests by enhancing our ability to identify and resolve a greater range of threats to our cyber infrastructure than would have been possible with the current state investment in cybersecurity. Michigan resolved 40 malware incidents affecting 590 state devices during the pilot.

What were the outcomes of the pilot? DHS decided as a result of the pilot that the EINSTEIN model would not scale well across the country. As a result, they turned the project over to the Multi-State Information Sharing and Analysis Center (MS-ISAC), a cyber-security group consisting of the 50 states.

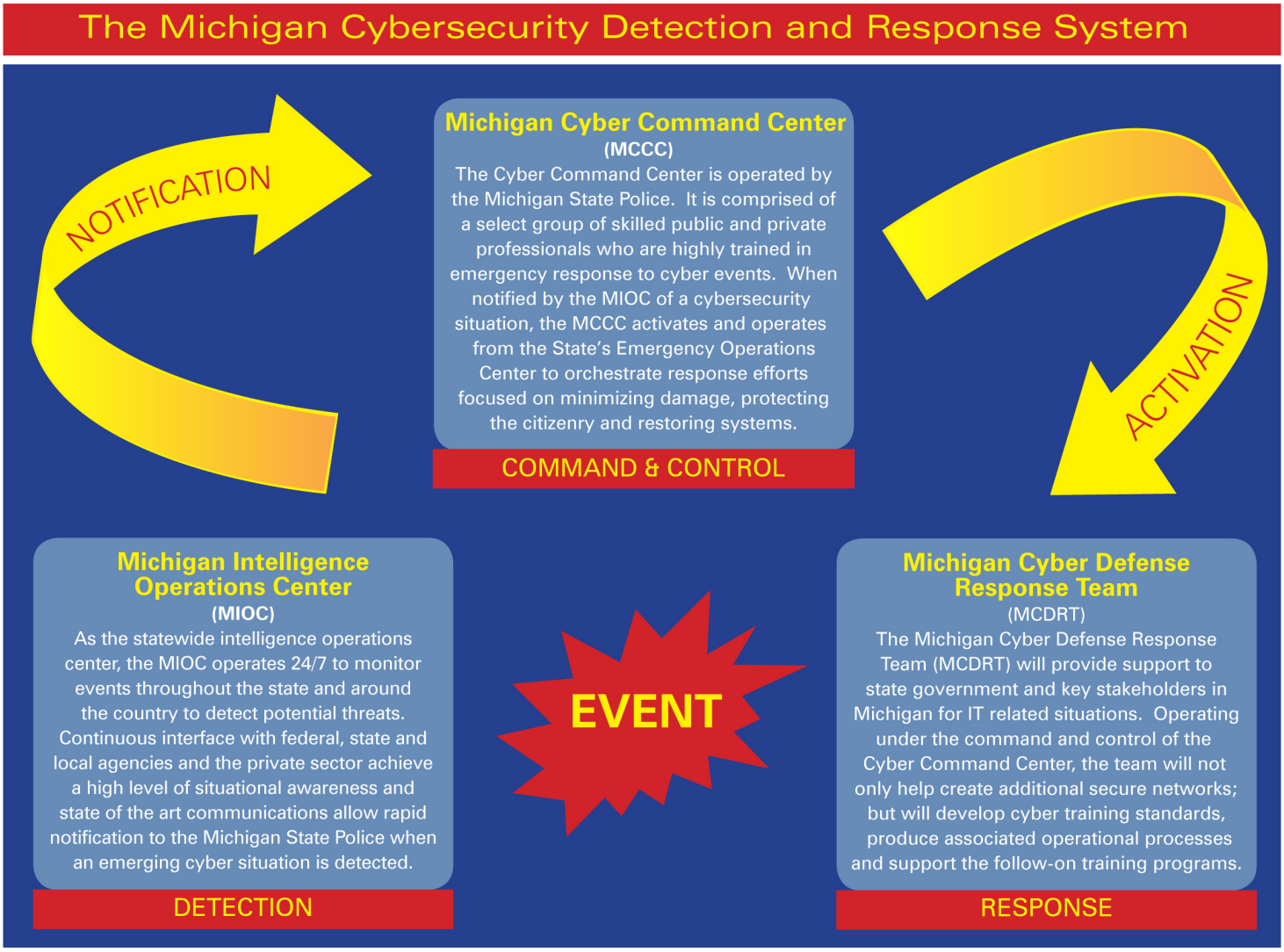
What is the ALBERT Program? It is a joint program between the MS-ISAC and DHS to bring an EINSTEIN-based program to the 50 states.

designed to provide the U.S. Computer Emergency Response Team (US-CERT) with network flow data that would help it identify suspicious anomalies. The pilot program was a success, and in 2011 Michigan became the first state to implement ALBERT, which is a more advanced protection partnership program with the MS-ISAC and DHS.

Early Detection and Rapid Response

The Michigan Intelligence Operations Center (MIOC) is Michigan's designated statewide Fusion Center. Operating 24-hours a day, seven days a week, the MIOC is a collaborative task force where local, state and federal agencies — as well as private sector partners — share information and intelligence related to homeland security.

The state is creating the Michigan Cyber Command Center (MCCC) to coordinate the combined efforts of cyber emergency responders. Under the direction of the Michigan State Police, the MCCC will be co-located with the State Emergency Operations Center. The MCCC will hold regular briefings, perform training, conduct exercises and will maintain dedicated resources to accommodate daily communication amongst state agencies. Regular communication channels will exist to provide state-wide visibility to current threats.



Michigan Cyber Initiative
Defense and Development for Michigan Citizens, Businesses and Industry

Control, Management and Restoration

Michigan needs to take appropriate steps to minimize and contain the effects of a cyber event and to reestablish normal operating conditions. To accomplish this, the state is creating a Michigan Cyber Defense Response Team to support state government and key stakeholders in Michigan. This team will function under the operational control of the Michigan Cyber Command Center and will undertake several key programs. These include establishing a response network that will use a "train the trainer" approach to inform a host of customers, improve network security and promote standards in training and operational processes to ensure best of class cyber emergency response.

Research

Michigan is no stranger to the innovations and developments in the information technology and Internet universe. Indeed, Michigan entrepreneurs have been at the forefront of Internet innovation since its beginning.

During the rapid explosion in Internet development and acceptance over the past two decades, a host of networking and security startups called Michigan their home base including:

History of Michigan and the Internet

In 1953, computers created in Ypsilanti by the classified Willow Run Laboratories which was operated by the University of Michigan were used to create the BOMARC missile. This nuclear capable surface-to-air missile was one of the most advanced technologies of its time.

Several years later, the University of Michigan established a computer science department and computing center, which made computers publicly accessible for general research and laid the ground work for Michigan's leadership role in computer technology.

As a response to the USSR launching Sputnik, the world's first artificial satellite, the Advanced Research Projects Agency (ARPA) was created to regain the strategic lead in science and technology. A decade later, the first design meetings for the ARPA network were held at the University of Michigan in Ann Arbor. The network grew to connect all ARPA's projects at universities and research labs across the country.

Meanwhile in 1966, Merit Network was created to connect Michigan's research universities. In the 1970's, Merit established one of the first research networks in the world. In 1987, Merit, IBM and MCI were awarded a National Science Foundation Grant to build and operate the NSFNET to connect America's supercomputing centers and regional research networks. During this time many of the Internet's core standards and technologies were developed in Michigan driven by Merit's Internet governance and standardization effort including:

> Border Gateway Protocol (BGP) – the core routing protocol for the Internet.
> Multipurpose Internet Mail Extensions (MIME) – transmitting documents through e-mail and the Web.
> Remote Authentication Dial In User Service (RADIUS) – centralized access to networks.
> Point-to-Point Protocol (PPP) – dial-up access to the Internet.
> In the 1990's the NSFNET commercialized to become the Internet.
> The University of Michigan continued to lead the development of key Internet protocols such as the Lightweight Directory Access Protocol (LDAP) and did key work on security protocols like Kerberos, IPSEC and NFSv4.
> As the Internet grew out of the NSFNET in the 1990's, Internet2 was created in Ann Arbor to develop the next generation of Internet technologies. Internet2 is the national research network that supports the most advanced research over the network as well as the most advanced research on the network.

ANS (UUnet, Worldcom),
Cybernet Systems,
Reactor Zero,
FirstVirtual, and
NetPOS

In addition to startup companies, well-established computer giants such as Google and Compuware have a significant presence in Michigan.

Key security systems and open-source protocols built in Michigan include OpenBSD and Open SSH, and the University of Michigan fostered local startups with its technology transfer initiatives. One example is Arbor Networks – a global leader in large network security systems.

More recently, other outside firms have recognized the state's positive environment for growing cybersecurity companies: Barracuda Networks and Greenhills Software are two examples of companies opening Michigan R&D facilities to tap into the local talent pools.

Education and Public Awareness

Even with leading edge technology, response networks and processes, a cyber ecosystem is only secure if those in the system are aware of and knowledgeable about cybersecurity.

Michigan has created a new Online Cyber Toolkit, to raise awareness and preparedness for all of the components of the ecosystem, and it is now available at www.michigan.gov/cybersecurity. This toolkit provides best practices and easy steps for safeguarding an environment with an appropriate toolkit from a trusted source. The new toolkit offers the chance to quiz yourself, downloads of posters and calendars as well as tip sheets on how to solve online problems. Examples of what is available include materials on:

Protecting Your Identity
Malware: Worms, Trojans and Viruses
Keeping Your Children Safe Online

Additionally, the following guides are being prepared for each sector and will be available in 2012.

Home Guide—will provide individuals and families with valuable information on protecting home computers, safeguarding against identity theft, and keeping children safe online—as well as calendars, screensavers and fun for kids.

Michigan will continue to partner with the federal government in education and training. Leveraging the NICE initiative, Michigan will be one of the first states to establish curricula and programs that achieve the objectives of that initiative.

Michigan Cyber Initiative Defense and Development for Michigan Citizens, Businesses and Industry

Business Guide—will address cyber security emerging trends and threats, security newsletters and alerts pertaining to computer viruses and other risks.

Government Guide—will provide cybersecurity information to the state workforce to enhance awareness, safeguard state systems and ensure continuity of operations—while addressing cybersecurity laws and issues related to privacy protection.

School Guide—will address the Michigan Cyber Safety Initiative which provides valuable online instructional materials for educating children in kindergarten through eighth grade, provides information for protecting children from such malicious activities as "cyberbullying" and "sexting," and other valuable educational materials.

Michigan Cybersecurity Education and Training

Economic opportunity and the successful development of our cybersecure ecosystem requires talent. To ensure Michigan's success, educators are working with their counterparts in the National Initiative for Cybersecurity Education (NICE). The mission of NICE is to "enhance the overall cyber security posture of the United States by accelerating the availability of educational and training resources designed to improve the cyber behavior, skills, and knowledge of every segment of the population, enabling a safer cyberspace for all". NICE plans to extend the scope of workforce training and awareness to include "students in kindergarten through post-graduate school" to achieve that goal.

Michigan will continue to partner with the federal government in education and training. Leveraging the NICE initiative, Michigan will be one of the first states to establish curricula and programs that achieve the objectives of that initiative.

Primary and Secondary Education in Online Safety

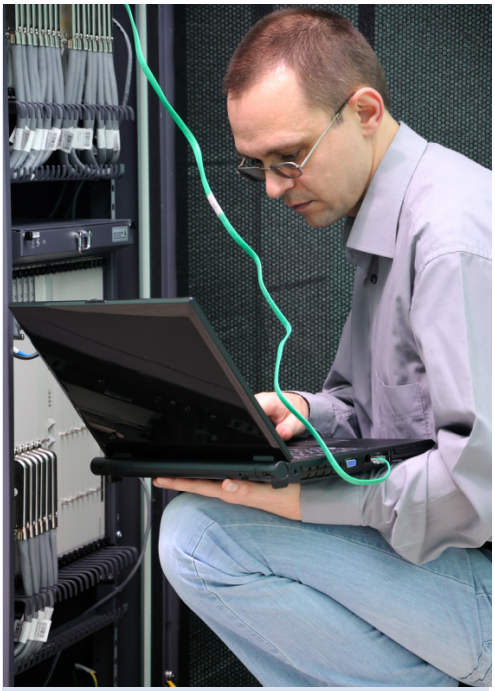
Michigan's Attorney General developed a Michigan Cyber Safety program for kids. The program is called "CSI" for "Cyber Safety Initiative." It involves free training for kids from kindergarten through 8th grade. (http://www.michigan.gov/csi)

Michigan CSI includes customized presentations for students in kindergarten through eighth grade that are offered by trained professionals from the Attorney General's Office. The program has been presented to more than 640,000 students in 455 school districts since its inception in the fall of 2007.

The 2011 program has been revised and updated to address

Continued emphasis on graduate level cybersecurity research and development (R&D) opportunities will attract students to strongly consider cybersecurity for their academic career focus.

Michigan Cyber Initiative
Defense and Development for Michigan Citizens, Businesses and Industry



Ensuring the capability of the cybersecurity workforce is a critical need across all economic sectors of the State. A standard cybersecurity competency framework is a prerequisite to effective human capital planning.

consequences associated with the increased prevalence of "cyberbullying" and "sexting" (the transfer of sexually explicit photos via cell phones), in addition to providing important safety tips about avoiding Internet predators.

Michigan CSI presentations include age-appropriate information about safe and responsible Internet use and communicate valuable lessons about Internet safety.

Secondary and Post-Secondary Education

Increasing the availability of programs with a cybersecurity focus in our college and university system will produce the expertise necessary to meet the needs of both public and private sectors. Therefore, an undergraduate focus on cybersecurity needs to be established in a greater percentage of the courses required for a bachelor or associate degrees in computer science, computer engineering, software engineering, information systems, and information technology. Cybersecurity expertise cannot be developed in a single course on security, but rather needs to be a foundation of all coursework. To meet these objectives, Michigan will:

- Explore public and private collaborations to create resource centers to support cybersecurity teaching and learning.
- Work in collaboration with Michigan universities to develop models for shared faculty, curricula, and virtual laboratories and make them easily accessible and publicly available.
- Implement state-of-the-art distance learning and online course materials.

College and University Research

From an educational, research and development perspective, Michigan has a proven track record of successfully using invested dollars for measurable results. The University of Michigan is a national leader in research and development funding.

The computer security research teams at Michigan universities are leaders in the field. Whether it is cutting-edge mobile security research being done at the University of Michigan, research into citizens' personal security behavior at Michigan State University or programs in cybersecurity at one of the five NSA Centers of excellence, Michigan leads the way.

Continued emphasis on graduate level research and development opportunities will attract students to strongly consider cybersecurity for their academic career focus. It is also a key part of developing the faculty capable of teaching future generations of cybersecurity students and innovators. To meet this objective, Michigan will identify and implement mechanisms that increase quantity and improve the quality of graduate research and development.

Michigan Cyber Initiative
Defense and Development for Michigan Citizens, Businesses and Industry

Cybersecurity Talent Development

To meet future needs, Michigan must have a robust, well-trained cybersecurity work force capable of serving the nation's needs. This will require multiple educational opportunities.

The standard definition of work force capability requirements is provided by a comprehensive set of standards being developed by the Committee on National Security Systems (CNSS). That set of CNSS standards specifies basic work force functional areas and the roles and professional career paths that are needed to carry out those functions. By implementing these standards across the public and private workforce, Michigan will be able to identify shortages and skill gaps for cybersecurity professionals.

To accomplish this, Michigan will:

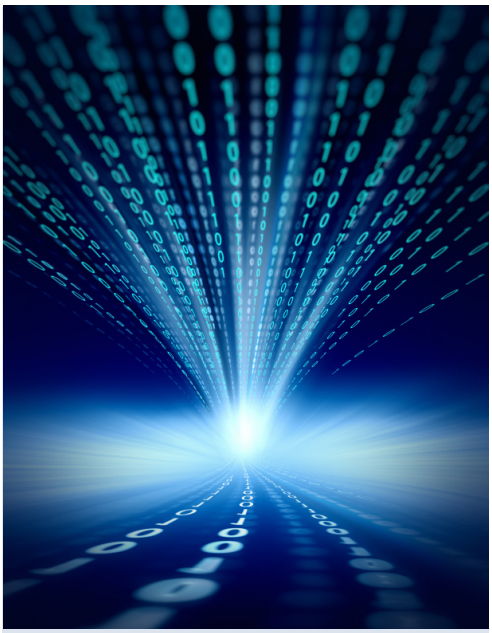
- Encourage public and private collaborations to utilize the DHS cybersecurity competency framework.
- Work with academia and industry to determine new workforce requirements from emerging technology and threats.
- Encourage the improvement and advancement of cybersecurity occupational certification programs.
- Establish a baseline for cybersecurity professionals across multiple industry sectors.

Michigan's talent development effort for cybersecurity will be a multidisciplinary one – focused not just upon technical knowledge but also upon the development of a "cyber-managerial skillset." Technical skills are always greatly in demand, but cybersecurity also relies increasingly upon inter-institutional partnerships and coordinated relationships.

Responding to this need, Michigan's cybersecurity talent development efforts focused upon both technical and managerial skills, aiming to provide a unique talent pool of "full-spectrum" cybersecurity professionals.

Through the Michigan Economic Development Corporation (MEDC), Michigan has developed several creative talent initiatives to grow this base of expertise locally. Cybersecurity will be a key feature of the following Talent Enhancement programs:

- **Shifting Gears**, a career-transition program for seasoned corporate professionals who want to pursue Michigan job opportunities in business growth sectors where they can leverage their business knowledge and experience in new ways.
- **MichAGAIN**, a campaign with the message, "Now is the perfect time to come back home." MichAGAIN helps talented individuals and growing businesses connect – and reconnect – with Michigan, sponsoring events in Boston, Chicago, Washington, DC, Cincinnati and



Beyond the formal education channels, we will also encourage and develop community programs such as the Cyber Citizenship Coalition of Washtenaw County and the International Information Systems Security Certification Consortium, Inc., $(ISC)^2$'s SCIPP security awareness certification program.

Michigan Cyber Initiative Defense and Development for Michigan Citizens, Businesses and Industry

San Francisco, with more to follow.

- **Global Michigan**, working to find new ways to encourage immigrants with advanced degrees to come to Michigan to work and live.
- **LiveWorkDetroit**, a MEDC program that connects Michigan's college graduates to new opportunities in Detroit and promotes the city as a post-graduation talent destination.

Beyond the formal education channels, we will also encourage and develop community programs such as the Cyber Citizenship Coalition of Washtenaw County and the International Information Systems Security Certification Consortium, Inc., (ISC)²'s SCIPP security awareness certification program.

Collaboration and Partnerships

A truly cyber resilient ecosystem is based on a holistic view of the environment and ensuring that it is working by strengthening existing partnerships and bringing all components of the ecosystem together to create a full Cyber Threat Alert Network.

The emerging field of cybersecurity has the potential to contribute significantly to Michigan's economic resurgence. The Michigan Cyber Initiative will enable existing Michigan businesses and startup enterprises to meet growing unmet demand in the cybersecurity market, providing business growth, investment and jobs for Michigan.

The Michigan Security Network (MiSN), a non-profit organization dedicated to accelerating growth in key homeland security focus areas, in partnership with MEDC has completed a comprehensive analysis of Michigan's cybersecurity growth opportunities. The findings have shaped the strategy for accelerating economic development by analyzing industry dynamics and trends and assessing Michigan's strengths and needs.

The following summarizes the action steps that can help the state remain a cybersecurity leader, secure its own networks, and grow the Michigan cybersecurity industry.

To be on the cutting edge of preparedness – and thus an attractive partner and preferred location for industry growth – requires a strong cybersecurity "culture," well-practiced cooperative instincts, managerial savvy, a willingness to explore innovative partnership opportunities, and ongoing political focus and attention.

Michigan Cyber Initiative
Defense and Development for
Michigan Citizens, Businesses and Industry

PART III –MICHIGAN'S UNIQUE CYBER INDUSTRY OPPORTUNITY

Cybersecurity Dynamics and Trends

Traditionally, most approaches to cybersecurity have focused upon the narrowly technical aspects of system vulnerability and specific threat-analysis or attack-defeat technologies. Increasingly, however, there is awareness that far more than mere technical competence is needed.

Cybersecurity issues must be addressed holistically and not as individual pieces and parts within various parts of numerous organizations and institutions. Cybersecurity requires collaborative relationships within and between all organizations. To be on the cutting edge of preparedness – and thus an attractive partner and preferred location for industry growth – requires a strong cybersecurity "culture," well-practiced cooperative instincts, managerial savvy, a willingness to explore innovative partnership opportunities, and ongoing political focus and attention.

Cybersecurity Economic Development Strategy

The biggest threat to our state's electronic infrastructure is cyber crime. While a critical focus for Michigan is securing public safety, the state must also continue to keep job creation at the forefront of the agenda.

To do that, Michigan will grow public-private cybersecurity partnerships, continuing to build the trust of private sector operators and promote compliance with state-of-the-art "best practices." The private sector excels at keeping pace with technology, but the overall cybersecurity ecosystem requires information-sharing and coordination among private entities and between the private and public sectors.

Michigan must play a lead role in improving such sharing and coordination, both within its borders and between state entities and the outside environment.

The state will continue to play a leading role in partnering with federal authorities. Key federal agencies have much experience with cybersecurity issues, and in many cases actively seek closer partnerships. Michigan's leadership and agility in this realm will keep the state at the forefront of intergovernmental cooperative cybersecurity.

Michigan will also continue to improve the safety and resilience of its own networks, as well as the ability of state systems to continue to restore critical services notwithstanding disruptive attack. By keeping its own networks secure and improving its ability to function as a cyber "first responder," Michigan will continue to be an attractive location for cyber-related businesses and a reliable partner in cybersecurity relationships.

Michigan will build public-private cybersecurity partnerships, continuing to build the trust of private sector operators and playing a facilitating and coordinating role in developing and promoting compliance with state-of-the-art "best practices."

Michigan Cyber Initiative Defense and Development for Michigan Citizens, Businesses and Industry

"Pure Michigan Business Connect is the cornerstone of a new toolkit for economic gardening we are developing that's built on Michigan's broad asset base of strong corporate enterprises, innovative entrepreneurs and rich technology resources," said Governor Rick Snyder.

Michigan also offers a wide range of programs to enable businesses to gain access to the capital they need to grow through the various stages of their development.

These programs will be critical to the growth of both start-ups and existing cybersecurity companies. Programs include the Michigan Capital Access Program, Collateral Support Program, and Loan Participation Program, as well as a variety of equity-based financing programs.

Entrepreneurial Support

Through the MEDC, Michigan has significantly increased support for our domestic entrepreneurial ecosystem, making Michigan a hot spot for innovation and entrepreneurial activities. Key programs that will benefit cybersecurity start-up ventures include:

- The Michigan Mentor Network, a program designed to match entrepreneurs with experienced mentors in the private and academic sectors.
- The Michigan Small Business and Technology Development Center (MiSBTDC) offers Michigan's most comprehensive entrepreneur and small business development program. Jointly funded by the MEDC and the US Department of Commerce, MiSBTDC provides counseling, training, research and advocacy for new ventures, existing small businesses and innovative technology companies. Services include technology counselors to provide more in-depth support and a road mapping tool that helps clients evaluate the direction of their technology, to departmentalize concepts and to chart strategic direction.
- A network of Smartzones and Business Incubators, including several with specific focus on high-tech growth industries.

Access to Capital — Pure Michigan Business Connect

Michigan recently launched Pure Michigan Business Connect, a $3 billion public-private initiative to strengthen Michigan's economic gardening. This program provides Michigan businesses innovative new ways to buy and sell, raise capital and connect with one another. Pure Michigan Business Connect matches people with resources and strengthens relationships to fuel economic growth.

Michigan also offers a wide range of programs to enable businesses to gain access to the capital they need to grow through the various stages of their development. These programs will be critical to the growth of both startups and existing cybersecurity companies. Programs include the Michigan Capital Access Program, Collateral Support Program and Loan Participation Program, as well as a variety of equity-based financing programs.

Michigan Cyber Initiative
Defense and Development for Michigan Citizens, Businesses and Industry

Michigan Defense Industry Assistance Center

As home to key defense and military procurement facilities, Michigan companies are perfectly and uniquely positioned to interact with the US armed forces in cybersecurity. The Michigan Defense Center's team of seasoned professionals, with their combined military backgrounds and government contracting experience, stand ready to help Michigan companies tap into the in-state market for military cybersecurity and other advanced technologies. This team works closely with a network of Michigan Procurement Technical Assistance Centers to prepare Michigan businesses to compete for government contracts by informing them of the opportunities, requirements and processes involved with becoming successful government contractors.

Product Beta Test Program

Startup cybersecurity companies begin with a great idea that they develop and prove in a lab or artificial environment. There is, however, no substitute for feedback from real users in a real environment. "Beta testing" is usually beyond the reach of startups. Most companies will not expend the resources needed to test and give good feedback on a technology from a little known company.

Michigan will fill this gap by creating a "Beta test" program for cybersecurity technology. The state will work with companies to deploy the pre-release products in segments of the state's IT infrastructure, thereby providing critical quality, suitability and effectiveness data.

Closing

Cybersecurity presents challenges that demand an unprecedented degree of inter-institutional competencies, coordination and collaboration. Building a successful approach will involve a comprehensive strategy that includes preserving the confidentiality of our data, the integrity of our systems and controlling availability only to authorized users through a three step process. Making Michigan the premier partner in and location for relevant business development lies not merely in technology but in managerial and collaborative excellence.

Michigan has a great history in this area—but an even brighter future. With proven successes not only in internal cybersecurity management but also in innovative public-private partnerships, Michigan will continue its leadership into the future of cybersecurity with the vision, drive and determination to address the cybersecurity needs of our nation for generations to come.

With proven successes not only in internal cybersecurity management but also in innovative public-private partnerships, Michigan will continue its leadership in the future of cybersecurity with the vision, drive and determination to address the cybersecurity needs of our nation for generations to come.